SECTION 5 TABLE OF CONTENTS

30 Jul 2004

Page

This page left blank intentionally.

5.0 DESIGN AND DEVELOPMENT

This section focuses on specific requirements an application developer must follow to ensure the release is compliant with NMCI standards. The objective of this guide is not to tell a developer how to develop a release, but to provide the essential information to support the Certification and Testing processes covered in Section 6.0. It also provides information on the different types of release deployments and to support each deployment scenario.

5.1 STANDARDS/PROGRAMMING PRACTICES

The NMCI architecture is designed to deliver an integrated family of networks, servers, and workstations configured to support the DON vision for seamless data connection. Therefore, the applications that reside on NMCI must be developed to comply with this architecture and standards.

5.1.1 Microsoft Development Standards

MS Windows 2000 application specifications are used in the development of releases hosted on NMCI in order to leverage the new technologies in MS Windows 2000, make releases more manageable and reliable, and reduce development costs.

Development Standards have two versions:

- **Desktop Specifications:** Refer to http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp

- **Server Specifications:** Refer to http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2ksrv/html/w2kserve.asp

This document details the requirements for desktop applications. The application must be compliant with the Windows 2000 installer service to ensure that the release can be cleanly installed/uninstalled, self-repaired, and rolled back on demand.

5.1.2 Programming Guidelines

Adhering to Microsoft guidelines ensures that releases run efficiently within NMCI. Microsoft provides the following specific tuning and optimization guidelines:

- Support Customization Through User Profiles
- No Memory Leaks
- Do Not Replace System Files
- Do Not Assume Computer Name or IP Address Equates to Single User
- DCOM Support
- Consider the Peripheral Hardware Environment

- Do Not Assume Persistence of Files in Temp
- Disallowing Multiple Instances of Some Applications
- Do Not Assume the Windows Shell
- Do Not Modify or replace the MSGINA.dll
- Negotiate Client/Server Connections Inside the System and Network
- Multilingual and International Usage Scenarios

5.2 PROGRAMMING STANDARDS FOR A TERMINAL SERVER PLATFORM

For applications to work well in a multiuser environment, certain programming standards must be used. Terminal servers host applications for multiple end users, but the application must be written so that user-specific information is not tied directly to a machine. For example, applications cannot use the Transmission Control Protocol/Internet Protocol (TCP/IP) address to uniquely identify a user because many users on a terminal server share the same address. Microsoft provides guidance on the following categories:

- Building a Terminal-Services-Aware Application
- Application Setup in a Terminal Services Environment
- Storing User-Specific Information
- Kernel Object Name Spaces
- IP Addresses and Computer Names
- Client/Server Applications
- Graphic Effects
- Peripheral Hardware
- Background Tasks
- Thread Usage

5.3 USER INTERFACE SPECIFICATIONS

Developers must consider user interfaces to applications to ensure that they meet current DoD policy, procedures, and standards (e.g., Defense Information Infrastructure Common Operating Environment - DII COE, C4ISR-AF, DITSCAP, and Section 508).

5.4 GROUP POLICY OBJECT (GPO)

The DON provides a layer of computer defense and control at the desktop by restricting access to the root and system directories, also known as NMCI Boundary 4 (B4) security. In other words, the desktop is “locked down.” The Navy sets GPO settings and policies and EDS implements them. In addition, EDS enforces contract SLA for the desktop by restricting certain user operations and desktop actions.

EDS administers the desktop and application authentication standards. Developers need to contact NNWC or EDS when creating or modifying applications for all GPO related issues. The following guidelines must be adhered to:

- Developers cannot update their Group Policy settings, either locally on the desktop or nonlocally at the AD level.

- Developers must modify releases to comply with GPO policies.

- Developers must go through recertification processes if their releases fail certification testing (GPO testing).

- Developers need to produce test plans/scripts that include the steps, data, and logical conditions necessary to trigger required authentication processes [e.g., Lightweight Directory Access Protocol (LDAP), AD, file sharing, file writes, etc.] to ensure that group policy, lockdown, and security areas are thoroughly examined during Certification in the EDS Applications Lab.

Releases may be permitted to run as a higher credentialed user. This allows the release to run at a user ID level that has the required GPO/security levels necessary, not as an individual user. Developers are required to program the command set, i.e., run as >userID, and incorporate this in the production environment (e.g., script, .bat file, etc.).

5.5 APPLICATION TESTING GUIDELINES FOR DEVELOPERS

The Applications Lab has developed a set of guidelines for developers to follow when designing applications. The guidelines are based on the Applications Lab experience in dealing with GOTS applications in the NMCI Environment. Guidelines are intended to improve the standardization of GOTS applications, with the following benefits:

- Increase the application compatibility within the NMCI environment
- Facilitate enterprise packaging.
- Reduce certification processing and troubleshooting time

Standardization is organized into three categories:

- Do's
- Don'ts
- Recommendations.

5.5.1 Do's

The Applications Lab requests that developers adhere to the following guidelines in order to significantly reduce the turnaround time of Packaging and Certification.

- Install applications in the C:\Program Files\Application Name folder, where Application Name is the name of the program.

  EXAMPLE: Install the program to C:\Program Files\USN AMP, where "United States Navy Aircraft Maintenance Program" is shortened to USN AMP. Support files may be

installed to other locations, but the main application must be installed in the Program Files folder.

- Store temporary files in the C:\Program Files\Application Name\Temp folder.

  The C:\Temp folder, although traditionally a common location to store temp files, is not supported in the NMCI environment due to its use of the enterprise software distribution system. Temporary files must reside in a location in which users have NTFS write or modify permissions. This temp folder within the application folder allows EDS personnel to quickly identify temporary files when troubleshooting.

  EXAMPLE: “C:\Program Files\USN AMP\Temp”

- Store configuration files (e.g., ini, cfg, sys, etc.) in either of two locations depending on the file protection/permission needs.

  Locating files in one of these two locations allows EDS personnel to quickly process applications for Packaging and Certification.

  – Store files that must or may be updated in the C:\Program Files\Application Name\Config folder.

    This unsecured folder allows applications to update the files during run-time.

    EXAMPLE: “C:\Program Files\USN AMP\config.cfg” (modifiable at runtime)

  – Store files that require a secured folder to prevent modification in C:\WINNT\System32\Developer\Application Name

    The secured folder prevents users from changing the files; however, it also prevent applications from making changes.

    NOTE: This is for files that do not need to be modified.

    EXAMPLE: C:\WINNT\System32\Developer\USN AMP\config.cfg” (not modifiable at runtime)

- Store data files (including saved data files and databases) at either the Local Machine or a shared folder in the network.

  – Local Machines:

    o **Single User:** Only one specific user may store and use these files. Store these files in the “My Documents” folder.

      EXAMPLE: C:\Documents and Settings\username\My Documents\USN AMP\Data

- **Multiple Users:** More than one person may use these files, which usually serve as a common source of data. Locate these files in the "C:\Program Files\Application Name\Data" folder.

  This allows EDS personnel to know where the application data files are stored and take proper measures to prevent those files from being updated or overwritten by the enterprise packaging system.

  EXAMPLE: "C:\Program Files\USN AMP\Data"

- **Shared Folders:** Use any shared path as long as the UNC discussed in this document is adhered to.

  EXAMPLE: "\\SPAWAR\SPOT\CMDSHARE\USN AMP\DATA"

- Install Application Shortcuts to the "C:\Documents and Settings\All Users\Start Menu\Programs\Application Name" folder.

  This ensures that the shortcuts are created in the Start Menu for all users and standardizes the location of shortcuts. The icon (.ico file) of the shortcuts can be of anything 'nonoffensive', but should not be the default Windows icon used when a file cannot be found. If an install package that installs shortcuts is used, care should be taken to ensure that only the "All Users" Start Menu shortcut is used.

  EXAMPLE: "C:\Documents and Settings\All Users\Start Menu\Programs\USN AMP\USN AMP.lnk"

- Provide test data with test plan for the application if data files (such as databases) are used.

  This allows for EDS personnel to conduct tests and be made aware of how the program should function correctly. Based on known test data inputs to the application, known outputs should be generated to ensure that the release functions properly.

- Verify the .msi package using a test program, such as ORCA.

  This affects MS Windows Installer (.msi)-based applications; e.g., applications that use the MS Windows Installer and have files ending with .msi file extension the enterprise packaging system cannot correctly package invalid .msi-based applications.

- Create a test login account and a password for applications that require the use of a login.

  If a test login account has not been provided, the Applications Lab rejects applications, as the certification test cannot be completely performed.

- Provide the License and/or Registration keys if the requires their use.

Without the information for those keys, the Applications Lab rejects the application, as the certification test cannot be completely performed.

- Completely fill out the RFS form for each application.

  See instructions for this form at the ISF Tools Database Users Guide on the ISF Tools Database Log-in page.

  The POC listed should be someone highly familiar with all aspects of the application.

- Provide a copy of the application manual or documentation to ISF personnel on how to take the following actions:

  – Install the application.
  – Test the application.
  – Operate the program.

- Provide an abstract (overview) on what the application is and does.

- Provide information (release notes) on known or acceptable errors and bugs.

  Any undocumented error that EDS personnel cannot solve would cause the Applications Lab to reject the application.

- Ship the applications on 3.5” floppy diskettes or CDs.

5.5.2 Don’ts

This section lists items that would cause the Applications Lab to reject the applications, or require substantial increased processing and turnaround time for application certification. The Applications Lab strongly recommends following this list to avoid immediate rejections and shorten the time for certification.

- Do not use desktop shortcuts (shortcuts that are on a user’s desktop screen). Desktop shortcuts created from applications are kept to a minimum in the NMCI environment. Users are allowed to create shortcuts themselves.

- Do not compress or zip the preinstalled application. Applications should be installed from diskette(s) or CD(s) without the need to uncompress or unzip. This is because machines used to package the application for enterprise deployment are not able to uncompress or unzip.

- Do not use the term “Beta” for versioning. An application that contains “Beta” in its version is automatically rejected, as this application is assumed to be a preproduction version.

  EXAMPLE: Use the numeric format for versioning (i.e., 2.00.2), instead of words (i.e., 2.00 Beta).

- Do not use modems. Do not include any functionality that requires the use of a modem.
- Do not support "Uninstall" or "Rollback" in the installation file executable. The NMCI enterprise application management system handles uninstall and rollback.
- Do not duplicate any Gold Disk applications or their functionality within the release: http://www.nmci-eds.com/downloads/Gold_disk_contents.pdf.

5.5.3 Recommendations

The Applications Lab provides the following tips to allow for quick certification and ease of troubleshooting or updating.

- Use good design programming standards and practices.
- Provide as much clear information as possible about the application. More information means an easier certification.
- Application configuration files should be in text format. Text-based configuration files allow for quick turnarounds in reconfiguring and preclude a complete repackaging of the application for enterprise deployment.

  EXAMPLE: An application designed for use at NAS Pax River is requested for use at NAS Lemoore, and is configured on a network. If the application uses a text-based configuration file, the Applications Lab can make the changes needed to the file within the NAS Pax River package without having to repackage and test the application. If the application has hard coded or embedded files in the application or encrypted, the program must be completely repackaged and certified.

  The nature and importance of the application determine how the developer uses the configuration files.
- Minimize the size of the application on local machines. (The developer must determine what is "small" or "large".) For a large application, two possible solutions may be used:
  - Use servers to support large programs or files (preferred solution).

    For example, a local machine (front end) has a small program to allow a user to use the large database (back end) on a server.
  - Use CDs either in a CD library (where possible) or on local machines (least preferred).
- Review the latest GPO revisions. Obtain the GPO information from the NMCI DAA.
- Schedule and coordinate the testing of the release with Applications Lab personnel to allow developer participation in the Packaging and Certification process.

5.6 NMCI INTERFACES

Interfaces to network infrastructure components are commonly identified by reading component specifications. Proper interfacing with enterprise infrastructures is required to ensure that the infrastructures continue to operate according to their original design and capacity.

This section identifies infrastructure interfaces, Application Program Interfaces (APIs), and specifications for the various types of applications that share the NMCI/IT-21 network environment. Developer responsibilities and common approaches to these interfaces are enumerated in an effort to protect, respect, and maximize the investment in the common enterprise network infrastructure. The goal for a developer should be to develop NMCI/IT-21/ MCTN applications that work securely and harmoniously with common network resources. Both NMCI and TFW participate in this object model through AD.

Information on Win32 API and the Microsoft Active Directory Service Interface (ADSI) model is available at http://www.microsoft.com/windows/reskits/webresources.

5.6.1 Windows 2000 Desktop Application Interface Specification

Microsoft provides the Windows 2000 standard desktop specification at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp.

This section describes the standard Windows 2000 APIs used in NMCI workstations and discusses NMCI use of Novadigm Radia (a software distribution system) and AD technologies that manage resource availability of both software and hardware, based on workstation or NMCI end user accounts.

Desktop applications developed for the NMCI Windows 2000 environment must undergo EDS certification processes prior to deployment within the NMCI environment. The NMCI environment, monitored by EDS, protects connected user workstations, data, and application servers if and only if developers or users interfacing with the network need guidance. Applications and users are controlled as objects and removed from participation in NMCI if they violate policy or specifications.

5.6.2 Microsoft Windows 2000 Server Interface Specification

Microsoft provides the Windows 2000 standard server specification at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2ksrv/html/w2kserve.asp.

This specification provides resources to attain Windows 2000 certification (including checklists) and receive the MS Windows 2000 logo. Meeting the MS Windows 2000 logo specification produces a release that is NMCI compliant. However, a developer may encounter situations in which applications must be developed which do not meet all MS Windows 2000 logo specifications. In cases where the GPOs, directory permissions, AD, firewall policy, and other settings cannot be met, the developer should contact the NMCI Help Desk for guidance.

5.6.3 Mobile Code

Mobile code is a powerful software tool that enhances cross-platform capabilities, sharing resources, and web-based solutions. Its use is widespread and increasing in both commercial and Government applications. The DoD uses mobile code in systems to support FAs, ranging from acquisition to intelligence to transportation. Mobile code is not restricted from use within NMCI. However, when used, it must be fully compliant with established DoD standards. Mobile code, unfortunately, has the potential to severely degrade DoD operations if improperly used or controlled. More detailed information on mobile code is available at http://iase.disa.mil/policy.html.

5.7 BOUNDARY/NETWORK INTERFACE SPECIFICATIONS

The type and strength of each security component is dependent upon the information protection requirements for a particular system. B1 reflects the Navy Marine Corps Enclave Protection Policy. B2 and B3 security mechanisms are flexible enough to meet the security requirements of various scenarios. Boundary configurations are tailored to provide the level of protection necessary to protect the integrity of NMCI and its users. NMCI also provides a wide-area IP backbone using DISA wide-area network (WAN) services with very high speed backbone network service (VBNS+) transport services. The Transport Boundary (TB) offers a secure encrypted intranet path between bases while imposing minimal restrictions on inter-base communications. Specific technical information on boundary requirements is available by contacting EDS IA personnel or the NMCI DAA.

Each system or application uses protocols to communicate between clients and servers. Many protocols and ports are associated with security vulnerabilities, and boundary policy reflects this. If an external application is compliant with B1 firewall policy, users within NMCI may access the application through the B1 boundary. To know if an application or system is compliant, its protocols, ports, and directions of activity must first be identified and characterized for assessment with respect to those of NMCI.

If an external system requires interaction not allowed by Navy/Marine Corps firewall policy, technical methods can obtain access through the boundary. The Navy/Marine Corps may choose to modify the baseline firewall policy to permit access to a system. Access may be possible through a virtual private network (VPN) path. A risk assessment must be prepared to determine whether a modification to firewall policy or the use of a VPN is acceptable. The NMCI DAA and local DAA use C&A documents to assess risks and make firewall policy modifications. A risk assessment does not need to be a one-at-a-time process; several applications can be considered simultaneously, if they run on shared servers and use the same ports/protocols.

5.7.1 Transport Boundary (TB)

The TB is a suite of network security components configured to provide WAN network security.

5.7.2 Boundary 1 (B1)

The B1 resides at the NOC and is designed to protect access to NMCI from the Nonsecure Internet Protocol Router Network (NIPRNET) and Secure Internet Protocol Router Network

(SIPRNET). This boundary protects NMCI users and services located in external networks (i.e., IT-21, MCTN, and Defense Information Systems Network - DISN). The B1 uses the Navy Marine Corps Enclave Protection Policy (NCEPP). The specifications for the B1 are available at https://www.infosec.navy.mil.

5.7.3 Boundary 2 (B2)

The B2 resides at the site and is designed to interface NMCI with the site legacy network. The B2 allows application reach back into the legacy network. The B2 is a transitional boundary that will no longer be employed once all Navy and Marine Corps networks migrate to NMCI. The specifications for the B2 can be obtained from the NMCI DAA (NNWC and HQMC C4).

5.7.4 Boundary 3 (B3)

The B3 is provided for use by COI operating within the NMCI network.

5.7.5 Boundary 4 (B4)

The B4 is composed of those measures taken to ensure secure operations and communications at the workstation or desktop level. This is accomplished through four primary methods: GPO settings, virus protection, intrusion detection, and compliance management.

5.8 NETWORK-RELATED APIS OTHER THAN STANDARD WINDOWS 2000 ADSI

MS ADSI may prove useful in realizing the enterprise benefits of AD. Further information is available at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_adsi.asp.

5.9 NMCI LOCKDOWN POLICY

NMCI lockdown policies disseminated through the AD, and enforced through GPOs, are highly restrictive settings that differ from the recommended MS Windows 2000 GPOs. Essentially, the application may write to its own area of a workstation disk with administrator privileges during install, but then must refrain from writing to restricted portions of the registry or other unauthorized areas of the disk at runtime.

5.10 SOFTWARE INSTALLATION

For pushed or remote installations, the installation script is run as administrator, but the same lockdown policy applies at runtime. Applications deployed to NMCI clients should be placed in a folder under the directory C:\PROGRAM FILES.

5.11 SCREEN SAVER

NMCI seats are set with the NMCI ISF screen saver. The screen saver activates after 15 minutes of inactivity and the user is prompted for a password to log back into the active desktop. The desktop user cannot change this.

5.12 TERMINAL SERVICE

From a “terminal service” perspective, “NMCI Thin Client” architecture supports MS Windows 32-bit applications. The Citrix components (Nfuse, etc.) can interoperate with the NMCI portal. This enables the launch of PC-based applications from the portal, display across the intranet, and the appearance of running locally while running remotely.

5.13 TESTING CONSIDERATIONS

Applications must successfully complete the Developer Test and Evaluation (DT&E), including the creation of test scripts and test cases. The application must be verified to work on an NMCI-certified workstation. Developers must describe the types of tests done in the NMCI Certification process:

- Will the application print?
- Will MS Office applications continue to operate?
- What are the considerations for prototype/pilot testing?
- What are the steps, data, and logical conditions necessary to trigger programmed authentication processes (LDAP, AD, file sharing, file writes, etc.)?

This ensures that group policy, lockdown, and security areas are thoroughly examined by the Certification and DT&E. Developers must ensure that logon IDs have the same access rights as end users, not developers. For detailed instruction on the DT&E, contact the EDS Applications Lab